McAfee Policy Auditor 6.0.0 software

Installation Guide

COPYRIGHT

Copyright © 2011 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Introducing McAfee Policy Auditor **4**

Product components 4

Audience 4

Conventions 5

Finding product documentation 5

Pre-Installation Tasks **6**

Preparation for installing the software 6

System requirements 6

Server requirements 6

Distributed repository requirements 10

McAfee Agent and ePolicy Orchestrator support 10

McAfee Policy Auditor agent plug-in platforms and support 10

Agentless audit support 12

Database considerations and support 12

Database storage requirements 14

Estimating database storage requirements 15

Database storage example and requirements table 15

Database storage requirements for File Integrity Monitoring 16

Database storage requirements for file versioning 17

Server requirements 18

Estimating database storage requirements 18

Installing McAfee Policy Auditor **19**

Install McAfee Policy Auditor on an MSCS cluster 19

Install McAfee Policy Auditor as an extension on ePolicy Orchestrator software 20

Update McAfee Policy Auditor content 20

Check in additional agent plug-in packages 21

Install the McAfee Vulnerability Manager extension 21

Uninstall McAfee Policy Auditor 22

Introducing McAfee Policy Auditor

McAfee® Policy Auditor automates the process required to conduct system compliance audits. It measures compliance by comparing the actual configuration of a system to the desired state of a system.

This guide provides system requirements for McAfee Policy Auditor software, and information about installing it as a managed product, as well as modifying, repairing, removing, and reinstalling the software.

Contents

- Product components
- Audience
- Conventions
- Finding product documentation

Product components

McAfee Policy Auditor software consists of several components that are used to create benchmarks, audit systems, and display results.

The McAfee Agent and the McAfee Policy Auditor agent plug-in do not need to be installed on systems that are audited by McAfee® Vulnerability Manager.

These are the McAfee Policy Auditor components as they appear in the user interface:

- **Benchmark Editor** — A utility used to enable, disable, create, and edit benchmarks. Each audit must contain at least one benchmark. Ideally, audits should contain only one benchmark.
- **Benchmark Editor Content Distributor** — Distributes content downloaded from McAfee Labs™ to systems.
- **Findings** — Manages findings, which help you understand why an audit check failed and information about how to fix the problem.
- **PACore** — The primary portion of the software that controls all other features.
- **PARollup** — Uses the rollup capabilities of ePolicy Orchestrator to collect summary information from registered ePolicy Orchestrator servers and show aggregated data.
- **Policy Auditor** — Handles policy and task management, audit schedules, and system management.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who are responsible for configuring the product options on their system, or for updating the product on their systems.

Conventions

This guide uses the following typographical conventions.

Book title or *Emphasis*	Title of a book, chapter, or topic; introduction of a new term; emphasis.
Bold	Text that is strongly emphasized.
User input or Path	Commands and other text that the user types; the path of a folder or program.
Code	A code sample.
User interface	Words in the user interface including options, menus, buttons, and dialog boxes.
Hypertext blue	A live link to a topic or to a website.
Note	Additional information, like an alternate method of accessing an option.
Tip	Suggestions and recommendations.
Important/Caution	Valuable advice to protect your computer system, software installation, network, business, or data.
Warning	Critical advice to prevent bodily harm when using a hardware product.

Finding product documentation

McAfee provides the information you need during each phase of product implementation, from installing to using and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User Documentation	1 Click **Product Documentation**. 2 Select a **Product**, then select a **Version**. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

Pre-Installation Tasks

Before installing McAfee Policy Auditor, you need to make sure your system is ready and meets the minimum software and hardware requirements. This section presents information to help plan and prepare your system before installing the software.

Contents

- Preparation for installing the software
- System requirements
- Database considerations and support

Preparation for installing the software

Complete these tasks before installing the McAfee Policy Auditor software.

1. Get the McAfee Policy Auditor software and documentation from the McAfee download site: https://secure.nai.com/us/forms/downloads/upgrades/login.asp
2. Review the release notes to identify last minute changes or known issues.
3. Verify that you have local administrator rights for the computer where you plan to install McAfee Policy Auditor.
4. Verify that your server or workstation meets the system requirements before you start the installation process. Refer to *System requirements* for details.
5. If you are installing a licensed version over an evaluation version of McAfee Policy Auditor, you must upgrade the license. The license is not automatically upgraded from an evaluation version.

System requirements

Verify that your server and systems to be audited meet these system requirements before you start the installation process.

NOTE: Unless otherwise specified, these are minimum requirements and are not optimal for performance. They apply only to McAfee Policy Auditor. You must also consider system requirements for any other products you are installing, such as McAfee Vulnerability Manager.

Server requirements

This section contains information you need to know before installing the McAfee Policy Auditor software, including hardware and software requirements.

Supported ePolicy Orchestrator software versions

One of these versions of ePolicy Orchestrator software must be installed and working before you install the software:

- ePolicy Orchestrator software version 4.5 Patch 5 or greater
- ePolicy Orchestrator software version 4.6

Domain controller requirements

The server must have a trust relationship with the Primary Domain Controller (PDC) on the network. For instructions, see the Microsoft product documentation.

Supported operating systems

McAfee Policy Auditor is installed as an extension of ePolicy Orchestrator software and runs on operating systems supported by that product.

For the most current information about supported operating systems, see this article in the McAfee KnowledgeBase: https://kc.mcafee.com/corporate/index?page=content&id=KB51569.

Microsoft operating system	Latest supported SP	ePO 4.5	ePO 4.6
Microsoft Windows 2008 Server Release 2, (64-bit) (**Standard**, **Enterprise**, and **Datacenter**)	—	Yes*	Yes
Microsoft Windows 2008 Server (64-bit) (**Standard**, **Enterprise**, and **Datacenter**)	2	Yes	Yes
Microsoft Windows 2008 Server (32-bit) (**Standard**, **Enterprise**, and **Datacenter**)	2	Yes	Yes
Microsoft Windows 2003 Storage Server	2	Yes	**No**
Microsoft Windows 2003 Server **Release 2**	2	Yes	Yes
Microsoft Windows 2003 Server **Release 2** (64-bit)	2	Yes	Yes
Microsoft Windows 2003 Server	2	Yes	Yes
Microsoft Windows 2003 Server (64-bit)	2	Yes	Yes
Microsoft Windows 2003 Web	1	Yes	**No**
Microsoft Windows 2008 Small Business Server Premium	—	**No**	Yes

* ePolicy Orchestrator software supports Microsoft Windows 2008 Server Release 2 Patch 1 and greater.

Browsers supported

ePolicy Orchestrator software runs on the most commonly-used browsers and can be accessed from anywhere on the network.

For the most current information about ePolicy Orchestrator software virtual infrastructure support, see this article on the McAfee KnowledgeBase: https://kc.mcafee.com/corporate/index?page=content&id=KB51569.

Browser	ePO 4.5	ePO 4.6
Microsoft Internet Explorer 9.0	**No***	**No***
Microsoft Internet Explorer 8.0	Yes	Yes
Microsoft Internet Explorer 7.0	Yes	Yes
Microsoft Internet Explorer 6.0	**No**	**No**

Browser	ePO 4.5	ePO 4.6
Microsoft Internet Explorer 5.5	**No**	**No**
Mozilla Firefox 4.0	**No***	**No***
Mozilla Firefox 3.6	Yes (with ePO 4.5 Patch 4 and greater)	Yes
Mozilla Firefox 3.5	**No**	Yes
Mozilla Firefox 3.0	Yes	**No**

* McAfee plans to test and provide support for Internet Explorer 9 and Firefox 4 in upcoming patch releases

Proxy servers

If you are using a proxy, bypass the proxy server:

1. From the Internet Explorer **Tools** menu, select **Internet Options**.
2. Select the **Connections** tab and click **LAN Settings**.
3. Select **Use a proxy server for your LAN**, then select **Bypass proxy server for local addresses**.
4. Click **OK**, then click **OK** again.

Ports needed by ePolicy Orchestrator software for communication through a firewall

ePolicy Orchestrator software uses ports to communicate with web browsers, SQL Server, managed systems, the network, and other portions of the software.

For the most current information about ports use by ePolicy Orchestrator software, see this article in the McAfee KnowledgeBase: https://kc.mcafee.com/corporate/index?page=content&id=KB66797.

This table shows the ports needed by ePolicy Orchestrator software versions 4.5 and 4.6 for communication through a firewall.

Port	Default	Description	Traffic direction
Agent to server communication port	80	TCP port opened by the ePolicy Orchestrator software server service to receive requests from agents.	Inbound/Outbound connection to/from the ePolicy Orchestrator software server/Agent Handler.
Agent communicating over SSL (4.5 and later agents only)	443	By default, agents should communicate over SSL (443 by default).	Inbound/Outbound connection to/from the ePO server/Agent Handler.
Agent wake-up communication port SuperAgent repository port	8081	TCP port opened by agents to receive agent wakeup requests from the ePolicy Orchestrator software server. TCP port opened to replicate repository content to a SuperAgent repository.	Outbound connection from the ePolicy Orchestrator software server/Agent Handler.
Agent broadcast communication port	8082	UDP port opened by SuperAgents to forward messages from the ePolicy Orchestrator software server/Agent Handler.	Outbound connection from the SuperAgents.

Port	Default	Description	Traffic direction
Console-to-application server communication port	8443	HTTPS port opened by the ePolicy Orchestrator software Application Server service to allow web browser UI access.	Inbound connection to the ePolicy Orchestrator software server.
Sensor-to-server communication port	8444	HTTPS port opened by the ePolicy Orchestrator software Application Server service to receive RSD connections. Also, used by the Agent Handler to talk to the ePolicy Orchestrator software server to get required information (like LDAP servers).	Inbound connection to the ePolicy Orchestrator software server. Outbound connection from remote Agent Handlers.
Security threats communication port	881	HTTP port hosted by McAfee Labs for retrieving security threat feed. Note that this port cannot be changed.	Outbound connection from the ePolicy Orchestrator software server.
SQL server TCP port	1433	TCP port used to communicate with the SQL server. This port is specified or determined automatically during the setup process.	Outbound connection from the ePolicy Orchestrator software server/Agent Handler.
SQL server UDP port	1434	UDP port used to request the TCP port that the SQL instance hosting the ePolicy Orchestrator software database is using.	Outbound connection from the ePolicy Orchestrator software server/Agent Handler.
Default LDAP server port	389	LDAP connection to look up computers, users, groups, and Organizational Units for User Based Policies.	Outbound connection from the ePolicy Orchestrator software server/Agent Handler.
Default SSL LDAP server port	646	User Based Policies use the LDAP connection to look up users, groups, and Organizational Units.	Outbound connection from the ePolicy Orchestrator software server/Agent Handler.

Supported virtual infrastructure software

ePolicy Orchestrator software runs on the most commonly-used virtual infrastructure software.

For the most current information about ePolicy Orchestrator software virtual infrastructure support, see this article on the McAfee KnowledgeBase: https://kc.mcafee.com/corporate/index?page=content&id=KB51569.

Virtual software	ePO 4.5	ePO 4.6
VMware ESXi 4.1	Yes	Yes
VMware ESX Server 4	Yes*	Yes
VMware ESX Server 3.5	Yes	Yes
VMware ESX Server 3.0.x	**No**	**No**
VMware Workstation 5.0	Yes	Yes
Microsoft Virtual Server 2005 R2 with SP1	Yes	Yes
Windows Server 2008 R2 Hyper-V	TBD	Yes
Windows Server 2008 Hyper-V	Yes	Yes
Citrix XenServer 5.5	**No**	Yes

* ESX 4.0 is supported with ePolicy Orchestrator software 4.5 Patch 1 and higher

Distributed repository requirements

Distributed repositories host copies of your master repository's contents. Consider using distributed repositories and strategically placing them throughout your network to ensure that managed systems are updated and to minimize network traffic.

As you update your master repository, the ePolicy Orchestrator software software replicates the contents to the distributed repositories. For more information on distributed repositories, see your appropriate ePolicy Orchestrator software product guides. Replication can occur:

- Automatically when specified package types are checked in to the master repository, as long as global updating is enabled.
- On a recurring schedule with replication tasks.
- Manually, by running a Replicate Now task.

Component	Requirement
Free disk space	100 MB on the drive where the repository is stored.
Memory	256 MB minimum.

McAfee Agent and ePolicy Orchestrator support

McAfee Policy Auditor software supports McAfee Agent versions 4.5 and 4.6. The available features depend upon the agent version and the ePolicy Orchestrator software version.

ePO server version	McAfee Agent version	Notes
4.6	4.6	Work together to support all legacy and new features.
4.6	4.5	Supports all legacy features. Some of the new features of ePolicy Orchestrator software version 4.6 and McAfee Agent4.6 are not available.
4.5	4.6	Supports all legacy features. Some of the new features of McAfee Agent4.6 are not available.
4.5	4.5	Work together to support all legacy features.

McAfee Policy Auditor agent plug-in platforms and support

The McAfee Policy Auditor agent plug-in supports a number of common enterprise platforms.

Operating system	X86 support	X64 support	Other processors	Notes
AIX 5.3 TL8 SP5			Power5, Power6	
AIX 6.1 TL2 SP0			Power5, Power6	
Apple Mac OS X 10.4	X	X	PowerPC	Universal binary
Apple Mac OS X 10.5	X	X	PowerPC	Universal binary
Apple Mac OS X 10.6	X	X	PowerPC	Universal binary
Windows 2000 Server	X			
HP-UX 11i v1			RISC	

Operating system	X86 support	X64 support	Other processors	Notes
HP-UX 11i v2			RISC	
HP-UX 11i v2 Itanium			RISC	
HP-UX 11i v3			RISC	
HP-UX 11i v3 Itanium			RISC	
Red Hat Linux AS, ES, WS 4.0	X	X		32-bit agent on 64-bit hardware
Red Hat Enterprise Linux 5.0, 5.1	X	X		32-bit agent on 64-bit hardware
Red Hat Enterprise Linux 6.0	X	X		32-bit agent on 64-bit hardware
Solaris 8			SPARC	
Solaris 9			SPARC	
Solaris 10			SPARC	
SuSE Linux 9	X	X		32-bit agent on 64-bit hardware
SuSE Linux Enterprise Server 10	X	X		32-bit agent on 64-bit hardware
SuSE Linux Enterprise Server 11	X	X		32-bit agent on 64-bit hardware
Windows 2000 Advanced Server	X			
Windows 2000 Professional	X			
Windows XP Professional	X	X		Native 32- and 64-bit agent
Windows Server 2003 Standard Edition	X	X		Native 32- and 64-bit agent
Windows Server 2003 Enterprise Edition	X	X		Native 32- and 64-bit agent
Windows Vista	X	X		Native 32- and 64-bit agent
Windows 2008 Server	X	X		Native 32- and 64-bit agent
Windows 7	X	X		Native 32- and 64-bit agent

Hardware and network requirements for Windows systems

These are the minimum requirements for McAfee Policy Auditor agent plug-in support on Windows systems:

Component	Requirements
Processor	Intel Pentium-class, Celeron, or compatible processor; 166 MHz processor or higher.
Free disk space for agent plug-in	300 MB.
Free disk space for other McAfee components	Sufficient disk space on client computers for each McAfee product that you plan to deploy. For more information, see the corresponding product documentation.
Free Memory	20 MB RAM.

Component	Requirements
Network environment	Microsoft or Novell NetWare networks. NetWare networks require TCP\IP.
Network interface card (NIC)	10 Mbps or higher.

Agentless audit support

Agentless audits allow you to audit systems that do not have the McAfee Policy Auditor agent plug-in installed. You can audit systems that do not have the agent plug-in by integrating McAfee Policy Auditor with McAfee Foundstone version 6.8 or McAfee Vulnerability Manager version 7.0.

To perform agentless audits, you must have a McAfee Foundstone or McAfee Vulnerability Manager server that is accessible over your network.

When determining how to implement agentless auditing, you need to consider your current ePolicy Orchestrator software installation, what version of McAfee Foundstone or McAfee Vulnerability Manager software you have installed, and your plans for upgrading your ePolicy Orchestrator software server.

Database considerations and support

McAfee Policy Auditor software, which requires a database, uses the ePolicy Orchestrator software server database by default. If no database is present, the installer offers to place SQL Server 2005 Express on your system.

Using McAfee Policy Auditor software with a database

Any of the following databases, if previously installed, meet the requirements for the software.

- SQL 2008 R2 Express
- SQL Server 2008
- SQL Server 2005 Express with Patch 2 or greater
- SQL Server 2005

CAUTION: If the minimum number of SQL Server licenses is not available after you install the SQL Server software, you might have a problem installing or starting the ePolicy Orchestrator software.

These tables provide additional information about your database choices and other software requirements.

Table 1: SQL server requirements

Database	ePO 4.5	ePO 4.6	Requirements	Notes
SQL 2008 R2 Express	No	Yes	Provides an option for automatically installing .NET Framework 2.0 SP2 or 3.5 SP1.	Available in 32-bit and 64-bit versions.
SQL 2008	No	Yes	Dedicated server and network connection	Needed if managing more than 5,000 systems.

Database	ePO 4.5	ePO 4.6	Requirements	Notes
			Local database server	If the database and McAfee Policy Auditor server are on the same system, McAfee recommends configuring your server to use a using a fixed virtual memory size that is approximately two-thirds of the total memory allotted for SQL Server. For example, if the system has 1 GB of RAM, set 660 MB as the fixed memory size for SQL Server.
			Licenses	A license is required for each processor on the system where SQL Server is installed. If the minimum number of SQL Server licenses is not available, you might have difficulty installing or starting the ePolicy Orchestrator software server.
SQL Server 2005	Yes	Yes	Dedicated server and network connection	Needed if managing more than 5,000 systems.
			Local database server	If the database and McAfee Policy Auditor server are on the same system, McAfee recommends configuring your server to use a using a fixed virtual memory size that is approximately two-thirds of the total memory allotted for SQL Server. For example, if the system has 1 GB of RAM, set 660 MB as the fixed memory size for SQL Server. SQL Server 2005 64-bit is supported only if it is installed on a separate system from the ePolicy Orchestrator software server.
			Licenses	A license is required for each processor on the system where SQL Server is installed. If the minimum number of SQL Server licenses is not available, you might have difficulty installing or starting the ePolicy Orchestrator software server.
SQL Server 2005 Express Patch 2	Yes	Yes	• .NET Framework 2.0 • .NET Framework 2.0 Service Pack 2	You must acquire and install .NET Framework 2.0 SP2. The Installer prompts you to install SQL Server 2005

Database	ePO 4.5	ePO 4.6	Requirements	Notes
				Backward Compatibility if it is not present.

Table 2: Additional software considerations

Software	Notes
Internet browser	See *Browsers supported*.
MDAC 2.8	If not previously installed, the installation wizard installs automatically.
SQL Server 2005 Backward Compatibility	If required, the installer prompts you to install it.
SQL Server 2005 Express	If no other database has been previously installed, this database can be installed automatically at user's selection.
Microsoft updates	Update the ePolicy Orchestrator software server and the database server with the most current updates and patches.
MSI 3.1	The installation fails if your server is using a version of MSI earlier than MSI 3.1.

Database storage requirements

When determining hardware needs for your organization, it is important to estimate the amount of database storage required to use McAfee Policy Auditor software.

McAfee has designed the software so that audit results consume the minimum amount of disk space. The amount of database storage you require depends on these factors:

- How frequently benchmark audits are performed.
- The number of systems audited.
- How long you want to retain audit results.

The tables used to calculate server and database requirements are based on tests of the software in the following distributed environment:

- **McAfee Policy Auditor server**
  - Four-processor, Intel Xenon 2.0GHz Core server
  - 4 GB of RAM
  - Windows 2003 Server 32-bit R2, Service Pack 2
  - RAID array 5 hard drive for local storage
- **Database server**
  - Four-processor, Intel Xenon 2.7GHz server with hyper threading
  - 4 GB of RAM
  - Windows 2003 Server 32-bit R2, Service Pack 2
  - SQL Server 2005, Service Pack 2
  - RAID array 5 hard drive for local storage

Effect of differential auditing results on database size

McAfee Policy Auditor increases database size an average of 760 KB of space per new system audited. The differential audits feature causes the increase in database size to decrease significantly after the first audit.

The Index Configuration server setting also affects the size of the database. If you use the Minimal Indexing option, the database will be smaller than if you use one of the other options.

The ultimate database size cannot be calculated accurately prior to deploying McAfee Policy Auditor, but can be estimated approximately 3 months after beginning a phased rollout. Use the database storage sizing estimates to determine the initial database size for new systems and new audits.

Estimating database storage requirements

You can estimate the average amount of hard disk space needed to store new McAfee audit results.

1. Determine the auditing requirements for your organization, including:
   - The number of audits you will be performing.
   - The frequency of each audit. For example, 20 audits once per quarter, 5 audits once per month, or one audit once per week.
   - The number of systems covered by each audit.
2. Use the example and the table in *Database sizing example and requirements table* to estimate the database space required for each audit.
3. Add the values for each audit. The sum is equal to the size of the database required to store the audit results for one year.
4. Determine the length of time you want to store the audits and adjust the database accordingly. For example, if you intend to store the audit results for two years, double the database size obtained in step 3. If you intend to store the audit results for six months, divide the database size by two.

Database storage example and requirements table

The requirements table for database sizing can help you calculate the the approximate disk space needed for your McAfee Policy Auditor database.

Requirements table for database sizing

Use this table to estimate the required size of your database. These estimates are based upon the average size of benchmark audit results. Your needs may vary.

Per system per year		1,000 systems	2,000 systems	5,000 systems	10,000 systems	20,000 systems	50,000 systems
Frequency	**Total audits**	**Database size (GB)**					
1 yearly	1	1	3	7	14	27	68
2 yearly	2	3	5	14	27	55	127
5 yearly	5	7	14	34	68	137	342
10 yearly	10	14	27	68	137	237	684
20 yearly	20	27	55	137	273	547	1,367
1 quarterly	4	5	11	27	55	109	273
2 quarterly	8	11	22	55	109	219	547
5 quarterly	20	27	55	137	273	547	1,367
10 quarterly	40	55	109	273	547	1,094	2,188

Per system per year		1,000 systems	2,000 systems	5,000 systems	10,000 systems	20,000 systems	50,000 systems
Frequency	**Total audits**	**Database size (GB)**					
20 quarterly	80	109	219	547	1,094	2,188	5,469
1 monthly	12	16	33	82	164	328	820
2 monthly	24	33	66	164	328	656	1,641
5 monthly	60	82	164	410	820	1,641	4,102
10 monthly	120	164	328	820	1,641	3,281	8,203
20 monthly	240	328	656	1,641	3,281	6,563	16,046
1 weekly	52	71	142	355	711	1,422	3,555
2 weekly	104	142	284	711	1,422	2,844	7,109
5 weekly	260	355	711	1,777	3,555	7,109	17,773
10 weekly	520	711	1,422	3,555	7,109	14,219	35,547
20 weekly	1040	1,422	2,844	7,109	14,219	28,438	71,094
1 daily	365	499	998	2,495	4,990	9,980	24,951
2 daily	730	998	1,996	4,990	9,980	19,961	49,902

Calculating database storage requirements

A corporation follows this policy for running audits:

- The company retains audit results for one year.
- One audit runs every three days on 2,000 systems. The table does not include this value, so we approximate this to two audits per week running on 2,000 systems.
- Five monthly audits run on 5,000 systems.
- One yearly audit runs on 150,000 systems. The table does not include this value, but it is equivalent to three yearly audits on 50,000 systems.
- Two quarterly audits run on 10,000 systems.

Calculate the approximate database size:

1 Look up the corresponding values in the table under *Requirements table for database sizing*, and note these results:

Audit frequency...	...running on number of systems	=	Database size (GB)
2 weekly audits	2,000 systems		284
5 monthly audits	5,000 systems		410
3 yearly audits	50,000 systems (3 × 68 = 204)		204
2 quarterly audits	10,000 systems		109

2 Calculate the total amount of space needed:

284 + 410 + 204 + 109 = 1,007 GB

Database storage requirements for File Integrity Monitoring

File Integrity Monitoring (FIM) allows you to designate a set of files to monitor for changes. McAfee Policy Auditor software monitors the MD5 and SHA-1 hashes of a file as well as the file attributes and permissions information. When a file changes, the McAfee Policy Auditor agent plug-in notes the change and sends an event back to the server.

The number of FIM events depends upon the number of files monitored and the frequency of changes to monitored files. The number of events is difficult to predict, but the impact to database storage is minimal.

Each FIM event adds approximately 3 kB to the database. If your organization generates one million events per month, the annual database growth is:

3 kB/event × 1,000,000 events/month × 12 months/year × 0.000001 GB/kB = 36 GB/year

Database storage requirements for file versioning

The File Integrity Monitoring feature of McAfee Policy Auditor software allows you to store up to six versions, including the file baseline, of text files from managed systems. The software does not support versioning for non-text files.

Version database sizing chart

This chart helps you calculate the database storage requirements for versioned files. The *Monitored File Size* column is the size of the file in megabytes for which you are storing version text. The *Versions* row is the number of file versions that you are storing.

Versions	2	3	4	5	6
Monitored File Size (MB)	**Database requirement per 1,000 systems (GB)**				
1	0.0573	0.115	0.172	0.229	0.287
2	0.0747	0.149	0/224	0.299	0.374
3	0.0983	0.196	0.294	0.393	0.492
4	0.138	0.276	0.415	0.553	0.691

Calculating versioning database storage requirements

A corporation follows this policy for maintaining file versions:

- Maintains file text for 5 versions of 2 MB files on 200,000 systems.
- Maintains file text for 4 versions of 1 MB files on 20,000 systems.
- Maintains file text for 3 versions of 4 MB files on 140,000 systems.
- Maintains file text for 6 versions of 3 MB files on 100,000 systems.

Calculate the approximate database size:

1. Look up the corresponding values in the table under *Version database sizing chart*, and note these results:

Versions	...running on number of systems (thousands)	Monitored File Size (MB)	Value from chart	=	Database size (GB)
5	200	(2)	0.299		59.80
4	20	(1)	0.172		3.44
3	140	(4)	0.276		38.64
6	100	(3)	0.492		49.20

2. To determine the database size, multiply the number of systems (in thousands) by the value that you obtained from the *Version database sizing chart*.
3. Calculate the total amount of space needed:

59.80 + 3.44 + 38.64 + 49.20 = 151 GB

Server requirements

This section contains information you need to know before installing the McAfee Policy Auditor software, including hardware and software requirements.

Supported ePolicy Orchestrator software versions

One of these versions of ePolicy Orchestrator software must be installed and working before you install the software:

- ePolicy Orchestrator software version 4.5 Patch 5 or greater
- ePolicy Orchestrator software version 4.6

Domain controller requirements

The server must have a trust relationship with the Primary Domain Controller (PDC) on the network. For instructions, see the Microsoft product documentation.

Estimating database storage requirements

You can estimate the average amount of hard disk space needed to store new McAfee audit results.

1. Determine the auditing requirements for your organization, including:
   - The number of audits you will be performing.
   - The frequency of each audit. For example, 20 audits once per quarter, 5 audits once per month, or one audit once per week.
   - The number of systems covered by each audit.
2. Use the example and the table in *Database sizing example and requirements table* to estimate the database space required for each audit.
3. Add the values for each audit. The sum is equal to the size of the database required to store the audit results for one year.
4. Determine the length of time you want to store the audits and adjust the database accordingly. For example, if you intend to store the audit results for two years, double the database size obtained in step 3. If you intend to store the audit results for six months, divide the database size by two.

Installing McAfee Policy Auditor

This version of McAfee Policy Auditor requires that you install one or more extensions in ePolicy Orchestrator software depending on the components you have purchased and the version of ePolicy Orchestrator software you are running.

Contents

- Install McAfee Policy Auditor on an MSCS cluster
- Install McAfee Policy Auditor as an extension on ePolicy Orchestrator software
- Update McAfee Policy Auditor content
- Check in additional agent plug-in packages
- Install the McAfee Vulnerability Manager extension
- Uninstall McAfee Policy Auditor

Install McAfee Policy Auditor on an MSCS cluster

Prepare ePolicy Orchestrator software installed on a Microsoft Cluster Service (MSCS) for installing McAfee Policy Auditor.

NOTE: For servers not on an MSCS cluster, you do not need to perform this task.

Task

For option definitions, click **?** in the interface.

1. Stop these ePolicy Orchestrator software services, then change their startup type to **Manual**.
   - McAfee ePolicy Orchestrator Application Server
   - McAfee ePolicy Orchestrator Event Parser
   - McAfee ePolicy Orchestrator Server
2. Install the software on each cluster member.
3. Before rebooting or using McAfee Policy Auditor, update the benchmark and check content with the *Update McAfee Policy Auditor content* task.
4. Restart these ePolicy Orchestrator software services, then change their startup type to **Automatic**.
   - McAfee ePolicy Orchestrator Application Server
   - McAfee ePolicy Orchestrator Event Parser
   - McAfee ePolicy Orchestrator Server
5. Test the cluster.
   a. Select the McAfee ePO Server group, then click **Bring Online**.

b Right-click any of the resources for the McAfee ePO Server group, then click **Initiate Failover**. The resources should fail and then come back online.

Install McAfee Policy Auditor as an extension on ePolicy Orchestrator software

Install the software on ePolicy Orchestrator software version 4.5 or 4.6 systems as an extension.

Task

For option definitions, click **?** in the interface.

1. Download the product zip files from the McAfee download site.
2. Click **Menu | Software | Extensions**.
3. Click **Install Extension**, then click **Browse**.
4. Select the PAPackage.zip file, then click **Open**.
5. If earlier versions of McAfee Policy Auditor software are installed, a dialog box asks whether you want to perform an upgrade of McAfee Policy Auditor. Click **Yes**, then click **OK**.
6. Review the *Install Package* information, then click **OK**.
7. Before rebooting or using McAfee Policy Auditor, update the benchmark and check content. See *Update McAfee Policy Auditor content* for instructions.

McAfee Policy Auditor appears in the **Managed Products** list under extensions and all the extensions installed for the software appear in the right pane.

Update McAfee Policy Auditor content

After installing McAfee Policy Auditor on ePolicy Orchestrator software, you must update the content before using the software or rebooting the system.

Task

For option definitions, click **?** in the interface.

1. To check in content, select **Menu | Automation | Server Tasks**.
2. Next to Update Master Repository, click **Run**. After running the server task, the content check-in requires approximately 30 minutes.
   - Do not restart your machine or use McAfee Policy Auditor or McAfee Benchmark Editor while McAfee ePO software is adding content.
   - Click **Menu | Reporting | Server Task Log** to verify that the new content has been checked in.

   NOTE: In ePolicy Orchestrator software version 4.6, you can also update the benchmark and editor content by clicking **Menu | Software | Master Repository**, then clicking **Actions | Pull Now** and following the Pull Now wizard. For more information, see *Using pull tasks to update the master repository* in the ePolicy Orchestrator software version 4.6 Product Guide.

Check in additional agent plug-in packages

When you install McAfee Policy Auditor, it automatically checks in agent plug-in packages for Windows, Mac OSX, and Linux to the Master Repository. If you have Solaris, AIX, or HP-UX systems, you need to separately check in these packages to the Master Repository.

For information on deploying the agent plug-in to systems in the System Tree, refer to *Install and uninstall the agent plug-in* in the McAfee Policy Auditor Product Guide.

Task

For option definitions, click **?** in the interface.

1. Download the appropriate agent plug-in zip files from the McAfee download site.
2. Click **Menu | Software | Master Repository**, then click **Actions | Check In Package**. The Check In Package wizard opens.
3. For Package type, select **Product or Update (.ZIP)**, then browse to and select the desired package file.
4. Click **Next**. The Package Options page appears.
5. Confirm or configure the following:
   - **Package info** — Confirm this is the correct package.
   - **Branch** — Select the desired branch. If there are requirements in your environment to test new packages before deploying them throughout the production environment, McAfee recommends using the Evaluation branch whenever checking in packages. Once you finish testing the packages, you can move them to the Current branch by clicking **Menu | Software | Master Repository**.
   - **Options** — Select whether to:
     - **Move the existing package to the Previous branch** — When selected, moves packages in the master repository from the Current branch to the Previous branch when a newer package of the same type is checked in. Available only when you select Current in Branch.
   - **Package signing** — Specifies if the package is signed by McAfee or is a third-party package.
6. Click **Save** to begin checking in the package, then wait while the package is checked in.

The new package appears in the Packages in Master Repository list on the Master Repository tab.

Install the McAfee Vulnerability Manager extension

The McAfee® Vulnerability Manager 6.8 and 7.0 extensions can be installed on ePolicy Orchestrator software version 4.5 or 4.6 environments.

NOTE: Install this extension only if you plan to integrate McAfee Vulnerability Manager with McAfee Policy Auditor. Otherwise, you do not need the extension.

Task

For option definitions, click **?** in the interface.

1. Download the appropriate McAfee Vulnerability Manager extension zip file from the McAfee download site, and store it on your ePolicy Orchestrator server.
2. Unzip the file to a convenient location. Read the release notes and the documentation, then double-click the **Setup** file to begin the installation.
3. Follow the instructions to complete the installation.

Uninstall McAfee Policy Auditor

You can remove the McAfee Policy Auditor program files to reinstall another version of the program or to completely remove the program.

NOTE: If you reinstall the software, McAfee strongly recommends that you restart your computer after you remove the files.

Task

For option definitions, click **?** in the interface.

1. Click **Menu | Software | Extensions**, select McAfee Policy Auditor in the Managed Products list, then in the right pane click the **Remove** link of each extension component. It is important to remove the components in the following order:
   - PA Rollup extension
   - Policy Auditor extension
   - Findings extension
   - Benchmark Editor Content Distributor extension
   - Benchmark Editor extension
   - PA Core extension
2. Click **Menu | Software | Master Repository**.
3. In the Actions column of the Audit Engine Content row, click **Delete** to remove the benchmark and check content.
4. To uninstall any remaining McAfee Policy Auditor agent plug-in packages, click **Menu | Software | Master Repository**.
5. Under the Name column, search for packages named McAfee Agent for <operating system>, such as McAfee Policy Auditor Agent for Windows. Under the Actions column, click **Delete** for each package.

Index

A

administrator rights 6
agent plug-in
  supported platforms 10
  Windows system requirements 10
agentless audit support
  Foundstone 6.8 12
  Vulnerability Manager 7.0 12
audience for this guide 4

B

browsers supported 7

C

components installed 4
conventions used in this guide 5

D

database requirements 12
distributed repositories, requirements 10
documentation
  product-specific, finding 5
  typographical conventions 5
domain controller requirements 6, 18

E

ePolicy Orchestrator
  database considerations and support 12
  database storage requirements 14, 15, 18
  database storage, file integrity monitoring 16
  database storage, file versioning 17
  ports used for communication 8

F

file integrity monitoring, database storage requirements 16
file versioning, database storage requirements 17
Foundstone
  install the ePO extension 21
  support 12
  Vulnerability Manager 12

I

install Policy Auditor
  additional agent plug-in packages 21
  as an extension 20
  on an MSCS cluster 19
install the ePO extension
  Foundstone 21
  Vulnerability Manager 21
installation requirements
  agentless audit support 12
installation requirements *(continued)*
  browsers supported 7
  database considerations 12
  database storage requirements 14, 15, 18
  database storage, file integrity monitoring 16
  database storage, file versioning 17
  distributed repositories 10
  domain controller requirements 6, 18
  hardware and networks 10
  McAfee Agent support 10
  Policy Auditor 6, 18
  Policy Auditor agent plug-in support 10
  supported operating systems 7
  supported virtual software 9

M

McAfee Agent, versions supported 10
McAfee recommendations 12
McAfee ServicePortal, accessing 5
McAfee Vulnerability Manager support 12

P

Policy Auditor
  additional agent plug-in packages 21
  components installed 4
  install as an extension 20
  install on an MSCS cluster 19
  server requirements 6, 18
  uninstall 22
  update content 20
Policy Auditor agent plug-in
  supported platforms 10
  Windows system requirements 10
ports used for communication 8
pre-installation, system requirements 6
proxy servers, browser bypass 7

R

repositories, requirements for distributed 10
requirements for installation
  agentless audit support 12
  browsers supported 7
  database considerations 12
  database storage 14, 15, 18
  database storage, file integrity monitoring 16
  database storage, file versioning 17
  distributed repositories 10
  domain controller requirements 6, 18
  hardware and networks 10
  McAfee Agent support 10
  Policy Auditor 6, 18
  Policy Auditor agent plug-in support 10
  server requirements 6, 18
  supported operating systems 7

requirements for installation *(continued)*
supported virtual software 9

S

ServicePortal, finding product documentation 5
SQL Server, supported versions 12
supported operating systems 7
supported virtual software 9
system requirements 6

T

tasks, pre-installation 6

U

uninstall Policy Auditor 22
update content 20

V

Vulnerability Manager, install the ePO extension 21